Data Confidentiality / Data Privacy Policy

Version 1.1

Document Information

Document Name	**Data Confidentiality Policy OR Data Privacy Policy**	**Version**	**1.1**
Date Created	18 APRIL 2024	**Released Date**	
Document No.	ISMS 011		
Classification	Internal		
Prepared By	Akshay Rane		
Reviewed By	Mahesh Tilave		
Approved By	P K X Thomas		

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without express written permission of the CEO of IRIS BUSINESS SERVICES LTD.

Revision History

Sr.No	Author	Date	Review details	Version Number
1	CISO	March 2024	No Change required	Ver 1.1

TABLE OF CONTENTS

1. Objective 4
2. Scope & Applicability 4
3. Definition & Glossary 4
4. Policy / Process 4
   4.1 Policy Definition 4
   4.2 Procedures 5
   4.3 Responsibility – IT Department / HR Department / Finance Department / Supply Chain 7
5. Data retention period 8
6. Data Retention Schedule 9
7. Non-compliance and consequences 11
8. Special Circumstances and Exceptions 11

1. Objective

The objective of Data Confidentiality or Data Privacy Policy (hereinafter referred to as 'Data Privacy Policy') is to set standards and/or framework for the usage and protection of confidential data related to the organization. Data Privacy Policy intends to communicate the organization's commitment in terms of protecting the privacy of user data and protection of consumer data within the organization. It is evidence of the organization's commitment to data protection principles.

2. Scope & Applicability

The Scope of Data Privacy Policy covers all employees, customers, suppliers, external consultants, partners, contractors and any other external entity. The policy defines the types of data and their appropriate usage.

3. Definition & Glossary

Term /Abbreviation	**Definition / Expansion**
IT	Information Technology

4. Policy / Process

4.1 Policy Definition

The Data Privacy Policy is designed to protect "personal data", which is "any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data". This expressly includes an individual's name, voice, image, identification number, electronic identifier, and geographical location. It also includes sensitive personal data and biometric data.

The Data Privacy Policy of the organization is set on the lines of the law to be compliant to standardize the use, monitoring and management of data. The main goal is to protect and secure all data consumed, managed and stored by the organization. The Data Privacy Policy includes all data stored by the core infrastructure of the organization, including storage and cloud services. It should help the organization ensure the security and integrity of all data—data-at-rest and data-in-transit.

4.2 Procedures

The Data Privacy Policy implementation is defined via procedures.
Information Technology (IT) department plays a vital role in implementing policy and ensuring adherence to the policy across the organization.
IT department, i.e. the IT Manager and/or chosen representative from the IT department, shall devise a comprehensive inventory cataloguing the storage locations of sensitive company data.
The comprehensive inventory should include the following analysis:

- HR systems data storing employee records in terms of name, gender orientation, designation, department, date of joining, compensation and wages details, payroll, health and retirement benefits.
- Employee record/s in the policy is defined as Personal data. Personal data is any information about an identified or identifiable person, known as a data subject, i.e. employee/s**.** Personal data includes any information that can be used to identify someone, alone or in combination with other information. This includes the employee/s name, date of birth, address proof and/or passport details, compensation & benefits, and educational qualifications- all of which can be utilized as identification of employee/s.
- Unstructured data residing in company equipment, remote servers and email accounts)
- Persons with a view or edit access to the data
- The volume of data ageing

The Data Privacy Policy of the organization is implemented by adhering to the following steps:

- Data Life Cycle Management – This refers to a framework that standardizes data processes in the organization, from data creation through storage and archiving until its final deletion.
- Data Risk Management – This includes identifying and assessing all risks and threats that may affect the data and thereby protecting the data confidentiality via undertaking necessary steps as may be deemed to be considered necessary.
- Data Back-up and Recovery – This includes the backup support mechanisms for data once data is created. All organization data is supported by a backup drive that is accessible in the case of an emergency, i.e. all systems failure.
- Data Access Management Controls – This includes that the data related to the organization shall be used only by authorized user/s. The records of the same shall be kept by the organization’s IT department.
- Data Storage Management – This includes tasks related to securely moving data on-premises or in external cloud environments. These may be data stores for frequent, high-performance access or archival storage for infrequent access.
- Data Breach Prevention - Data breach prevention measures are implemented for the purpose of preventing unauthorized access to data. The goal is to

avoid external malicious viruses or internal threats from gaining unauthorized access to information and systems. Cyber security measures are put in place for the purpose of preventing attacks on internal networks, network perimeters, data-in-transit, and data-at-rest. Typically, these measures include data encryption, implementation of antivirus software, protection against ransomware, perimeter security hardware and software, and access management software.

- Monitoring and Reviewing - Monitoring and reviewing processes help organizations gain visibility into data activities, risks and controls, helping improve protection and respond to threats and anomalies. Monitoring and reviews may also be necessary to meet compliance requirements. Ongoing monitoring provides visibility into all aspects of the data lifecycle, including data creation, storage, transmission, archiving, and destruction. These activities offer essential evidence for internal and external auditors that examine controls for data protection and management.

The organization upholds the highest responsibility in data collection from the subscribers if any, and the data received for job applications.
Therefore data collected from subscribers, if any, job applicants, employee/s, data related to products, new product development and innovations, finance, supply chain and any other data shall be treated with confidentiality.
All data shall be treated in the following manner:

- All data shall be processed within its legal and moral boundaries.
- All data shall be protected against illegal and unauthorized access.
- All data shall be protected against any unauthorized or illegal access by internal or external parties.
- Data shall not be communicated informally.
- The data shall not be stored for more than the specified time.
- Data shall not be distributed or transferred to organizations, states or countries that do not have adequate data protection policies.
- Data shall not be distributed to any other parties other than the agreed upon (exempting legitimate requests from law enforcement authorities)
- Let the employee/s and/or parties involved from whom the data is being collected and keep them informed of how, i.e. how, the data shall be processed/used and who has access to it.

4.3 Responsibility – IT Department / HR Department / Finance Department / Supply Chain

- The IT Manager must formulate an effective governance strategy to keep track of inward or outward data flow.
- The IT Manager and the Supply Chain Manager shall have to maintain oversight of third-party service providers and data processors since the Data Protection Law considers the collecting party responsible for the safeguarding of personal data even if the information has subsequently been shared with other parties.
- HR Manager/s and/or Business Head/s of the organization are strictly responsible for adhering to and ensuring the culture of data confidentiality with respective teams. Building an enterprise-wide appreciation of good information security practices requires a combination of senior-level buy-in and a commitment to continuous learning.
- The IT Manager should constantly be vigilant in maintaining IT security and controls similar to the adoption of information security frameworks or the ISO International Standard for Privacy Information Management.
- Adoption of effective data breach response measures

5. Data retention period

- Personal information (i.e. information that relates to identifiable individuals) can be lawfully retained only for as long as retention is necessary to achieve the legitimate business purpose for which the data is collected and processed. Ensuring compliance with this requirement means that IRIS and its employees must proactively manage personal information retention periods.
- Beyond personal information, IRIS has business requirements to retain other information, such as confidential information that is required for the normal conduct of our hospitality business or for accounting, tax or legal reasons.
- In some cases, such as in connection to accounting, tax or actual or potential litigation, IRIS is required to retain data, including personal information, for specified periods of time.
- In summary, where the law mandates retention and/or prescribes specific retention periods for specific types of data, the obligation to retain the data will prevail over the limitations concerning the retention of personal information.
- For example, even after an employee has left the organization, IRIS may need to keep information about the ex-employee to provide references or to defend legal claims like the employees PF details. However, if there is no objective reason that justifies keeping personal information, such data should be deleted or anonymized. The business process owner who is responsible for collecting the data is also responsible for ensuring that he data is anonymized or deleted in accordance with this policy. For further guidance on acceptable methods to anonymize or delete data please contact the Data Privacy and Protection Office who will help direct / answer your queries.

6. Data Retention Schedule

- Your local legal function will be able to provide you with the retention periods that apply in your local market. If you are unclear about the retention periods that apply to data for which you are responsible, please contact the Data Privacy and Protection Office.
- Retention periods generally are counted from the date the underlying matter ceases to be active. For example:
    - A contract would be held for the specified period after its expiration or termination.
    - A tribunal/court record would be retained for the specified period after the conclusion of the case.
    - Guest records would be retained for the specified period after expiry of the customer relationship.
    - Employee records would be held for the specified period after the termination of the employment relationship.
- If a particular record is in two categories, the longer retention period applies. Data retention schedule:

Record Type category	Retention Period	Reason
Book of Accounts	6 years	
Payroll and salary records	7 years	
Employee tax records	8 years	
Reports on employee performance review meetings and assessment interviews (e.g. evaluations, employment application forms of successful applicants, copies of academic and other training received, employment contracts and their amendments, correspondence concerning appointment, appraisals, promotions and demotions, agreements concerning activities in relation to the works council, references and sick leave records)	3 years or 1 year after audit, whichever is later	
HR data like Provident fund information of employees	7 years	
CCTV	3 years	
Emails	5 years	Archive after 1 year
Subject Access Requests	5 years	
Electronic marketing data – customers	5 years	
Booking data, check-in data, special requests data	For as long as the guest remains a customer	
Financial data and credit card information	For as long as it is necessary to process the transaction, including any queries which may arise.	

Loyalty scheme information	For as long as the guest is an active participant in the loyalty scheme. .	
Contact information of guest.	As long as the guest remains a customer.	
Health data special requests, or in connection with gyms or spas	1 year	
Information provided via tour operators and other 3rd parties. (Guest lists etc.).	7 years	
Guest details of current registration number, details of driving licence, details of passport (physical/electronic)	7 years	
System logs	18 months	

7. Non-compliance and consequences

In the event of non-compliance with Data Privacy Policy, the concerned Department Manager/s and/or concerned parties involved shall be suspended and/or terminated and/or legal action shall be taken towards parties involved in non-compliance.

8. Special Circumstances and Exceptions

In the event the Manager/s are unable to comply with the Data Privacy Policy due to challenges that involve specific situation/s or circumstances, then the party and/or parties involved shall be exempted in writing by the management from any legal action.